UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/889,557	07/27/2001	Marc Girault	211526US2PCT	7668

22850   7590   01/18/2006

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
PERUNGAVOOR, VENKATANARAY

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*27 December 2005*</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>*8-11, 13 and 14*</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>*8, 9, 13 and 14*</u> is/are rejected.

7)☐ Claim(s) <u>*10-11*</u> is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

Response to Arguments

1. The Applicant's arguments regarding Schneier being silent with respect to the use of

    Chinese Remainder theorem in authentication process is incorrect see enclosed NPL[1]. As

    Schneier discloses the use of Chinese Remainder theorem to "speed up" the calculating

    of keys used in authentication. And further, the Applicant is reminded it is not required

    that the prior art disclose or suggest the properties newly-discovered by an applicant in

    order for there to be a prima facie case of obviousness. See In re Dillon, 919 F.2d 688, 16

    USPQ2d 1897, 1905 (Fed. Cir. 1990). Moreover, as long as some motivation or

    suggestion to combine the references is provided by the prior art taken as a whole, the

    law does not require that the references be combined for the reasons contemplated by the

    inventor. See In re Beattie, 974 F.2d 1309, 24 USPQ2d 1040 (Fed. Cir. 1992); In re

    Kronig, 539 F.2d 1300, 190 USPQ 425 (CCPA 1976) and In re Wilder, 429 F.2d 447,

    166 USPQ 545 (CCPA 1970).

2. The Applicant's arguments regarding the use of Chinese remainder theorem in the

    present invention is suggested by Shamir. As Shamir is suggestive of the reduced of x, e

    and n in $y = x^e \pmod{n}$ see Page 4 Ln 18-22 & Ln 44-55. Shamir suggests n being

    factored into p and g, also talks of a small value of x in order to provide for benefits in

    size being smaller and faster calculation. And further Shamir discloses the choosing of e

    based on the n and x, and thus if n and x are being modified so must e in order to provide

    for significant "wraparound". Shamir anticipates the reduction of the instant invention by

taking the memory and computing power needed to carry out this calculation in account

and the reduction is suggested as one of these methods see Page 4 Ln 24-29.

3. The Applicant's arguments regarding p and g being similar size is fully met by Shamir

see Page 4 Ln 18-22, where Shamir discloses the p and g being of similar size, either bit

length or on the same order(i.e. 10s). And further Shamir mentions the v_j being restricted

to v_j, -v_j, $2v_j$, -$2v_j$ and easily specified in a directory because of the choice of similar size p

and g.

Response to Amendments

Claim Rejections – 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth
> in section 102 of this title, if the differences between the subject matter sought to be patented and the
> prior art are such that the subject matter as a whole would have been obvious at the time the invention
> was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability
> shall not be negatived by the manner in which the invention was made.

5. Claim 8 rejected under 35 U.S.C. 103(a) as being unpatentable over EP0325238 to

Shamir in view of Scheiner.

6. Regarding Claim 8, Shamir discloses an authentication process involving a first device,

which possesses a public key v and a secret key s, these keys being related by an

---

[1] Schenier, Bruce. "Public-Key Algorithms: RSA." Applied Cryptography: Protocols, Algorithms and

operation modulo n, where n is an integer, the modulus n being specific to the first device

and a second device, which knows the public key v, these devices being provided with

means to exchange zero-knowledge information and carry out cryptographic calculations

on this information, some calculations being carried out modulo n, the process being

characterized in that the modulo n operation is of the kind $v=s^{-t}(mod\ n)$ being a parameter

see Abstract & Page 4 Line 33-49. But, Shamir does not disclose the use of Chinese

Remainder method. However, Scheiner discloses the use of Chinese Remainder's

method see NPL[2]. It would be obvious to one having ordinary skill in the art at the time

of the invention to the Chinese Remainder method in the invention of Shamir in order to

speed up calculations as taught in Scheiner see NPL[3].

7. Regarding Claim 9, The "first device selects at least one integer at random ranging

between 1 and n-1 and calculates at least one parameter x equal to $r^{t}(mod\ n)$, then at least

one number c that is at least one function of the at least one of a parameter and a

message, and sends the at least one number c to the second device, the second device

receives the c, selects one number e at random and sends this question to the first device,

the first device receives the question e, carries out at least one calculation using the at

least one number e and the secret key s, the result of the at least one calculation yielding

at least one answer y and sends the at least one answer y to the second device. The

second device receives the answer y, carries out one calculation using the public key v

Source Code in C. New York: John Wiley & Sons, 1996. pp 470.
[2] Schenier, Bruce. "Mathematical Background: Number Theory." Applied Cryptography: Protocols,
Algorithms and Source Code in C. New York: John Wiley & Sons, 1996. pp 249-250.
[3] See footnote 1.

and the modulus n, and checks with a modulo n calculation that the result is coherent with the received at least one number c" is met by Shamir see Page 2 Line 44 - Page 3 Line 41.

8. Regarding Claim 13, The "a message signature process configured for a device provided with a public key v and a secret key s, the public and private keys being related by a modulo n calculation, where n is an integer, which is specific to the device, the process utilizing means configured to calculate at least one number c that is a function of a message M to be signed, configured to calculate at least one number y that is a function of the secret key s, and configured to transmit the numbers y and c that are the signature of the message and the message M, wherein the modulo n operation is $v=s^{-t}(mod \ n)$, t being a parameter" is met by Shamir see Abstract & Page 4 Line 33-49 & Page 2 Line 44 - Page 3 Line 41.

9. Regarding Claim 14, The "device selects an integer r at random between 1 and n-1, calculates a parameter x equal to rt (mod n), calculates at least one number e that is a function of parameter x and the message M to be signed, calculates the at least one number y using its secret key s, said at least one number y being a function of numbers r and e, and transmits the numbers c and y as the signature" is met by Shamir see Page 2 Line 44 - Page 3 Line 41.

Allowable Subject Matter

10. Claim 10 and 11 would be allowable if rewritten to overcome the rejection(s) under 35

U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the

limitations of the base claim and any intervening claims.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the

advisory action. In no event, however, will the statutory period for reply expire later than

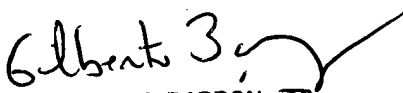SIX MONTHS from the mailing date of this final action.

12. Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Venkatanarayanan Perungavoor whose telephone number

is 571-272-7213. The examiner can normally be reached on 8-4:30. If attempts to reach

the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron

can be reached on 571-272-3799. The fax phone number for the organization where this

application or proceeding is assigned is 703-872-9306.

13. Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free).

<div style="text-align:right">

Venkatanarayanan Perungavoor
Examiner
Art Unit 2132

</div>

i/P
5/20/2005

<div style="text-align:right">

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

</div>